DOCUMENT RESUME

ED 180 466 IR 007 940

TITLE	International Barriers to Data Flows: Background Report. Prepared for the Use of the Committee on Interstate and Foreign Commerce, House of Representatives, and Its Subcommittee on Communications, Ninety-Sixth Congress, First Session.
INSTITUTION	Congress of the U. S., Washington, D. C. House Committee on Interstate and Foreign Commerce.
REPORT NO	House-Comm-Print-96-IFC-19
PUB DATE	Apr 79
NOTE	24p.
AVAILABLE FROM	Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402
EDRS PRICE	MF01/PC01 Plus Postage.
DESCRIPTORS	Background; *Communications; *Information Dissemination; International Organizations; *International Relations; *Laws; *Privacy
IDENTIFIERS	Communications Industry; Computer Industry; Europe; *Transborder Data Flows

ABSTRACT

This document is a staff study on a potentially major problem in international communications: the erection of international barriers to the free flow of data communications. Background and analysis are provided on (1) the European computer/communications industry; (2) national privacy laws of Sweden, Norway and Denmark, West Germany, France, Great Britain, and the United States; and (3) transborder data flows--major issues and action in international organizations, i.e., the United Nations, Nordic Council, Council of Europe, European Economic Community, and the Organization for Economic Cooperation and Development. A framework for future consideration concludes the report. (JD)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED180466

96th Congress
1st Session

COMMITTEE PRINT

COMMITTEE PRINT 96-IFC 19

INTERNATIONAL BARRIERS TO DATA FLOWS

Background Report

U S DEPARTMENT OF HEALTH
EDUCATION & WELFARE
NATIONAL INSTITUTE OF
EDUCATION

THIS DOCUMENT HAS BEEN REPRODUCED EXACTLY AS RECEIVED FROM THE PERSON OR ORGANIZATION ORIGINATING IT. POINTS OF VIEW OR OPINIONS STATED DO NOT NECESSARILY REPRESENT OFFICIAL NATIONAL INSTITUTE OF EDUCATION POSITION OR POLICY

PREPARED FOR THE USE OF THE

COMMITTEE ON INTERSTATE AND FOREIGN COMMERCE
HOUSE OF REPRESENTATIVES

AND ITS

SUBCOMMITTEE ON COMMUNICATIONS

NINETY-SIXTH CONGRESS

FIRST SESSION

APRIL 1979

U.S. GOVERNMENT PRINTING OFFICE
44-668 WASHINGTON : 1979

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402

IR007940

COMMITTEE ON INTERSTATE AND FOREIGN COMMERCE

HARLEY O. STAGGERS, West Virginia, *Chairman*

JOHN D. DINGELL, Michigan
LIONEL VAN DEERLIN, California
JOHN M. MURPHY, New York
DAVID E. SATTERFIELD III, Virginia
BOB ECKHARDT, Texas
RICHARDSON PREYER, North Carolina
JAMES H. SCHEUER, New York
RICHARD L. OTTINGER, New York
HENRY A. WAXMAN, California
TIMOTHY E. WIRTH, Colorado
PHILIP R. SHARP, Indiana
JAMES J. FLORIO, New Jersey
ANTHONY TOBY MOFFETT, Connecticut
JIM SANTINI, Nevada
ANDREW MAGUIRE, New Jersey
MARTY RUSSO, Illinois
EDWARD J. MARKEY, Massachusetts
THOMAS A. LUKEN, Ohio
DOUG WALGREN, Pennsylvania
ALBERT GORE, JR., Tennessee
BARBARA A. MIKULSKI, Maryland
RONALD M. MOTTL, Ohio
PHIL GRAMM, Texas
AL SWIFT, Washington
MICKEY LELAND, Texas
RICHARD C. SHELBY, Alabama

SAMUEL L. DEVINE, Ohio
JAMES T. BROYHILL, North Carolina
TIM LEE CARTER, Kentucky
CLARENCE J. BROWN, Ohio
JAMES M. COLLINS, Texas
NORMAN F. LENT, New York
EDWARD R. MADIGAN, Illinois
CARLOS J. MOORHEAD, California
MATTHEW J. RINALDO, New Jersey
DAVE STOCKMAN, Michigan
MARC L. MARKS, Pennsylvania
TOM CORCORAN, Illinois
GARY A. LEE, New York
TOM LOEFFLER, Texas
WILLIAM E. DANNEMEYER, California

W. E. WILLIAMSON, *Chief Clerk and Staff Director*
KENNETH J. PAINTER, *First Assistant Clerk*
BRIAN R. MOIR, *Professional Staff*
BERNARD J. WUNDER, JR., *Associate Minority Counsel*

SUBCOMMITTEE ON COMMUNICATIONS

LIONEL VAN DEERLIN, California, *Chairman*

JOHN M. MURPHY, New York
TIMOTHY E. WIRTH, Colorado
MARTY RUSSO, Illinois
EDWARD J. MARKEY, Massachusetts
RONALD M. MOTTL, Ohio
AL SWIFT, Washington
THOMAS A. LUKEN, Ohio
ALBERT GORE, JR., Tennessee
HARLEY O. STAGGERS, West Virginia
(Ex Officio)

JAMES M. COLLINS, Texas
JAMES T. BROYHILL, North Carolina
CARLOS J. MOORHEAD, California
MARC L. MARKS, Pennsylvania
SAMUEL L. DEVINE, Ohio
(Ex Officio)

HARRY M. SHOOSHAN III, *Staff Director/Counsel*

LETTER OF TRANSMITTAL

WASHINGTON, D.C., *April 30, 1979.*

Hon. HARLEY O. STAGGERS,
Chairman, Committee on Interstate and Foreign Commerce,
U.S. House of Representatives,
Washington, D.C.

DEAR MR. CHAIRMAN: Attached is a staff study on a potentially major problem in international communications, the erection of international barriers to the free flow of data communications. The study was prepared by Kathleen Casey, Minority Staff Assistant, under the supervision of Ronald D. Coleman, Associate Minority Counsel. Undoubtedly, this study is the only comprehensive report on this very recent issue.

Since the comprehensive communications legislation being considered by our Subcommittee addresses this issue, it would be helpful to the Members of the Committee to publish this study as a Committee Print.

Sincerely,

LIONEL VAN DEERLIN, *Chairman,*
Subcommittee on Communications.

CONTENTS

	Page
Letter of Transmittal	III
I. Introduction	1
II. Abstract	2
III. Background and analysis	2
A. The European computer/communications industry	2
B. National privacy laws	5
1. Sweden	6
2. Norway and Denmark	7
3. West Germany	8
4. France	9
5. Great Britain	10
6. United States	10
C. Transborder data flows	11
1. Major issues	11
2. Action in international organizations	14
a. United Nations	15
b. Nordic Council	16
c. Council of Europe	16
d. European Economic Community	17
e. Organization for Economic Cooperation and Development	17
IV. Framework for future consideration	18

INTERNATIONAL BARRIERS TO DATA FLOWS

Background Report

I. Introduction

The term "transborder data flows" refers to the electronic transmission of data across political boundaries for processing and/or storage in computer files. The establishment and use of transborder data networks has burgeoned as a consequence of a complex and ever-growing mix of communications technologies, providing an answer to transactional and recordkeeping needs. Declining costs and continuing refinements, in turn, continue to create new markets and new demands.

As the infrastructure of the post-industrial society, the problems arising from information technology are those of abundance, in contrast with the problems of shortage in such resources as energy or arable lands. It has the potential for becoming the essence of the advancement of productivity and knowledge. Conversely, it can become the stock for regressive trade restraints: either result could follow from designs to cooperatively control the spill-over effects of transborder data flows. A range of proposals is emerging in this relatively new field of international regulation.

The commerce of information has in fact become the foundation of new rights and duties on the part of nations for which there are few precedents in international law. Because of this, and despite the fact of its leadership in world markets, the United States does not have a free hand in the matter of regulating transborder data flows.

This report is a discussion of the issue and dealings with it by various countries and international organizations. Because the issue of regulating data flows has come about as a result of their prevalence, Section III(A) attempts to impart an understanding of the economic and technological motivations compelling their increasing applications. The discussion focuses also on the hand that American industry has had in the development of the industry abroad. Attention then turns in Section III(B) to the formulation of various kinds of national privacy laws both proposed and enacted. This subject is not usually detailed in writings on transborder data flows. Here, however, it places the problems surrounding transborder data flows in perspective. Inasmuch as national privacy laws are also attendant to the abundance of data technology, and are consequently an outgrowth of some similar social concerns, they are a precedent to transborder regulation proposals that are discussed in Section III(C). All of this sketches groundwork for establishing a frame of reference in Section IV by which the United States might become involved in the cooperative regulatory effort. Specific options are not furnished, however, since the U.S. has hardly grasped an awareness of the very difficult problems of transborder data flow regulation, much less a consensus on their imminence and applicability to U.S. interests. This analysis may, it is hoped, help to direct some attention to further research and to an ultimate resolution of the matter.

II. Abstract

National governments and international organizations are examining some potentially harmful impacts arising from the free international flow of information. Apprehension is particularly acute in Europe because of the fact that so much data processing, transmission, and storage there is frequently performed in a country other than where the data is collected and used, or where the concerned data subject resides. Individual governments have enacted or are contemplating restrictions designed to safeguard the security of personal data. The majority of them are seeking to extend these protections to data transmitted and processed outside of their boundaries.

While the protection of personal information has provided the initial incentive for national data regulation, when applied to transborder data flows, several more issues arise. These issues are the effects of transborder data flows on assorted economic, political, and cultural interests. Information is becoming more and more regarded as a critical asset, "the wave of the future." Protectionist instincts could, it is felt, drive foreign business out of certain countries and regions, permitting local firms to cultivate their markets in data processing. Restrictions on transborder flows apparently also equate with cultural integrity, an expulsion of disturbing foreign influences. These motivations form part and parcel of a contemplation of state sovereignty.

National governments and international organizations are examining these issues and also the potential harmful spillover effects arising from regulation designed to resolve them. In particular, economic stakes ride on unfettered access to modern computer/communications networks. Restrictions on business operations, particularly those of American-based multinationals and service firms, could stifle overall development. Most European governments seek to establish a regional or international framework to harmonize disparate laws and insure reciprocity. As a matter of enacting such a framework, all of these different interests may be analyzed as a matter of competing goals; when balanced satisfactorily, they can assimilate and strengthen an institutional basis for the international processing industry. On the other hand, treaties may be based on temporizing over these goals. Worse, an international perspective may be scuttled: individual nations or groups of nations would be free to legislate a crazy quilt of conflicting law.

An intensive cooperative effort is being lobbied on the part of individual governments, industry, and such institutions as educational and research foundations and trade associations. However, even with its substantial stakes in the matter, the United States has not taken a clearcut stand. Action is considered crucial as work in Europe is advancing quite far without American input.

III. Background and Analysis

A. The European Computer/Communications Industry

The convergence of computers and telecommunications has made data communications one of the fastest growing industries in the world.

It is estimated that 40 percent of the total world market exists outside of the United States and Canada. The most dramatic increases in data communications are expected to occur in the major industrialized countries of Europe and Japan; and share is expected to increase to 50 percent during the next decade, as more countries introduce or expand their facilities.[1] The linkage of computer/communications networks, accommodating flows of data across borders, secures advantages to the operations of private businesses and industries around the world. To a growing extent, data services are also being used in the public sector.

Multinational enterprises account for a significant share of transborder data flows. These include banks, airlines, hotels, car rental and credit card companies, insurance and medical reference organizations, and computer service bureaus, as well as international news services and major broadcasting companies. Many of these networks are owned and operated by firms for their internal use. There is also a wide array of "community networks" which are owned or leased by groups of users for special purposes. Among the most important private user networks is SITA, a high-speed flight reservation circuit which connects 160 airlines with 6,000 branches in 90 countries, and SWIFT, a worldwide inter-bank telecommunications financial service.[2]

Many commercial offerers lease or sell facilities for these kinds of dedicated applications. Small localized firms, too, are also employing service bureaus which transmit and process information abroad. All of these privately-owned networks may randomly cross borders, or are organized on a regional basis, as in Scandinavia.

The public sector has lagged behind the business community in using transborder data networks. Until recently, it has not engaged much more than a flow of research and statistics providing economic, demographic, and other characteristics of countries, although a new pattern is emerging which indicates that individual governments are formalizing cooperative exchanges of data.

International organizations are sponsoring networks and centralized data banks for an array of purposes. The United Nations has several systems in operation in its various agencies, and such world-wide networks as UNISIST, a scientific and technical information center. The European Space Research Organization (ESRO) has a well-known network referencing a wide array of science and technology. The Council of Ministers of the European Economic Community (Common Market) has directed the establishment of a European scientific and technical information network to add to the already existing international systems.

In the area of social welfare, a more mobile labor force is changing the handling of tax and social insurance files pertaining to thousands of individuals. The Common Market group and the Scandinavian countries are developing data banks for neighboring governments and by some even as far away as Canada. There are also formal interchanges of criminal investigation data, and an international passport system is underway.[3] The common carriers of ten European countries

[1] U.S. Department of Commerce, "U.S. Service Industries in World Markets" (Washington, December 1976), p. A-75.

[2] Organization for Economic Cooperation and Development, Data Bank Panel, "The Transborder Movement and Protection of Data, Principles and Guidelines," mimeo (Paris, Jan. 18, 1977), pp. 5-6.

[3] OECD, Computer Utilization Group, Report to the Data Bank Panel, "Transborder Data Flows: Issues and Implications," mimeo (Paris, May 10, 1975), pp. 6-7.

44-668—79——2

have organized a group called Eurodata Foundation, whose purpose is to study the feasibility of a regional electronic mail network. Also, the Common Market is implementing a packet switched service to be called EURONET.

For the most part, information is exchanged between the common carrier data communications networks, generally known as the Postal Telephone and Telegraph Organizations (PTTs). These are generally either government agencies or government owned and controlled corporations.

Within their countries, several European common carriers are refining their domestic service to accommodate anticipated demand. For instance, the French PTT is introducing two data networks, CYCLADES and TRANSPAC, and the United Kingdom is developing an experimental packet-switched data service for country-wide access.

A crucial element in the European computer network configuration is the fact of American trade expertise in both services and facilities. U.S. computer firms began commercialization of hardware and services earlier than most foreign corporations, which appear to have been too preoccupied with the development of their home markets to penetrate foreign markets. The outlook for the U.S. computer services industry is generally judged to be quite good, with forecasts of compound annual growth rates ranging from 15 to 20 percent through 1980.[4] In data communications on the other hand, U.S. companies have difficulty instituting networks. As noted above, much of the potential market exists in Europe, but these companies face foreign government-sponsored or financed competition. Consequently, communications exports are largely receipts by the U.S. international record carriers (telephone, telex, etc.); although consulting and managerial know-how is dispensed abroad, which can lead to exports of telecommunications equipment.

Many of the multinational users of transborder data flows are American affiliates (e.g., Massey-Ferguson, Shell, CitiBank, Holiday Inn, etc.), which often prefer to integrate their data processing systems with the parent firm using the same compatible American technology. This provides a market for American-based computer/communications services firms (e.g., Tymnet, Telenet, IBM, Honeywell, Xerox). While also contributing their share of traffic to data flows, the purpose of these affiliates is to provide this on-site support in managerial and consulting services and hardware. Their customers include firms from the overseas locale. In some cases, foreign-based firms actually keep their computer operations in the continental United States, a service of American companies. American affiliates provide some service for networks like SITA, SWIFT, etc. In many cases, they may have a minority ownership in one or another of the foreign computer/communications firms.

Judging from the ubiquitousness of data communications and computers, their use has penetrated and transformed methods of planning, management and administration in many walks of life. In the next 10 to 15 years, it is expected that it will be quite common in Europe for the computers located in the various parts of the region to guide and control long transportation chains and distribution in large industrial concerns (including the sub-contractor network).

[4] Dept. of Commerce, op. cit., n. 1, p. A-90.

By 1985, an estimated 1.73 million data terminals will have been installed. 815,000 will be directly contributing to data traffic to PTT lines and networks; 915,000 will operate on in-house systems.[5] As an estimate of volume, these figures represent a twelve-fold increase for Europe as a whole,[6] while estimates for individual countries vary.[7]

This seemingly irreversible trend toward increasingly large-scale data flows is compelled by technological development and economic factors. Soon, users of any capacity may be able to choose among custom-made computers, and digital techniques have significantly improved the efficiency of data transmission. Transmission facilities will continue to increase in number, providing improved methods and greater capacity. Transmission distance has already become a minor factor for wire and microwave networks. Satellites have made this factor trivial.

Technology has also found ways of tailoring the quality of systems to meet specific preferences for security, convenience, and centralized management. Cooperating organizations such as banks, airlines, and insurance companies can pull resources into a central data base or community network. Regular processing can be assured in the event of breakdown or interruption through contact with firms that use similar applications. Telecommunications technology has become the solution also for centralized control requirements particularly in multinational firms. Day-to-day operations of subsidiaries attain greater efficiency through interconnection with a central data bank than is possible with manual files. Consequently, firms feel free to expand without fear of upsetting control over research, marketing and economic records, etc.

These technological improvements, interacting with price competition, induce lower costs. There are strong economic advantages in replacing manpower with computers and data networks; in several years the use of a system may cost only a fraction of the salary of the terminal operator. Hence, use of data communications and processing will increase as technological feasibility improves and costs lower. The process feeds on itself: economic and technological refinements parallel demand for services and, in turn, stimulate that demand.

B. NATIONAL PRIVACY LAWS

Originally, data processing applications were confined to tasks in fields of research and planning which do not affect people directly. Computers were huge machines used in data processing centers. When computers and data networks made their appearance in daily administration, their impacts came to be felt by the individual. While he or she may feel that, on the whole, technology dealing in information and knowledge has advanced the "quality of life," each has an interest in controlling personal information that is held by others. This ambivalence is rooted in fundamental social mores and ideas of personal liberty. Recordkeeping regulations of the manual era cannot adequately protect the integrity of the great volume of personal information in automated networks and files. Unauthorized access to paper

[5] OECD, Data Bank Panel, op. cit., n. 2, p. 5.
[6] Id.
[7] E.g., a thirty to fiftyfold rise in traffic volume is guaged for Sweden during the next decade. Swedish Ministry of Defense, "The Vulnerable Computer Society," Stockholm, 1976, p. 1. See also reprint, "Transnational Data Report, (TDR)" vol. 1, No. 5 (Nov. 1978), pp. 13-20.

files has always been a substantial risk. However, the chances of abuse of computerized systems increases because of the greater capabilities of the medium and because of factors such as the length of transmission channels and the concommitant danger of interception. Electronically, it is more difficult than with manual files to protect information from unauthorized access and to prevent and detect offenses. Currently, France, Sweden, Norway, Denmark, West Germany, Canada, and the United States have national privacy acts. Sweden, Norway, Denmark, and West Germany extend their laws to data transported, processed and accessed outside of the country.

Since privacy is rather undefined as a legal concept, the goal of seeking safeguards has had to balance with that of assuring a flow of information relevant to the rights and needs of the community as a whole. These competing goals have had to be confronted in devising both the standards of the law and its enforcement methods.

Standards most often addressed are the methods of data collecting, their relevance and accuracy for the purpose for which they are collected, the time period for which they are stored, the security methods used, and reasonable access and correction procedures for whomever the data may apply. The enforcement mechanisms most often implemented or considered are various penalties for violations, self regulation on the part of data network and data bank operators, the registration or licensing of data, and in some cases, data banks and networks, and periodic government inspection of data and/or of the hardware. It is important to note that data protection proposals are often meant to protect the integrity of private organizations (i.e., business or trade associations), as well as of the individual. This prevents the interception of confidential commercial information such as income records, trade secrets, etc.

Although the legal provisions contain similar directives, national differences do exist. The weight given one or another legislative goal differs among individual countries according to the sophistication of the technology and its degree of penetration. It also hinges on the degree of public arousal and the status of existing criminal and civil law. The national laws of the Scandinavian countries are a particular case in point.

1. Sweden

As early as 1766, Swedish constitutional law and practice have recognized a principle of free access to public records.[8] Its government has developed a system of large, centralized data banks and the exchange of data between government agencies and to the public is relatively uninhibited in comparison to other western governments. This tradition, however, did conflict with security requirements; and a Swedish Data Act was enacted in 1973. Sweden's was the first of any comprehensive privacy law.

The act applies to computerized personal information processed in the private and public sectors. Its effectiveness is governed by permit standards implemented by a Data Protection Board. In general, the Board grants permits to maintain personal registers unless it finds that it would result in "undue encroachment on the privacy of

[8] Frits Hondius, "Emerging Data Protection in Europe" (Amsterdam, North Holland Publishing Co., 1975), p. 4.

individuals".[9] Thus, permission to register personal religious or political beliefs is granted only exceptionally, and there are graded restrictions of other kinds of personal information that may be processed in the private sector. The Board also specifies the purpose of the register in question, what personal information may be included, and, where appropriate, may limit the time period during which the register is kept. There are also stipulations to provide access—the right of the individual to inspect a record that concerns him or her, to revise incorrect or incomplete data, and to control disclosure to third parties. Significantly, the Data Act requires that exporters of data about Swedish citizens receive permission from the Data Protection Board.

2. Norway and Denmark

Recently enacted privacy legislation in other Scandinavian countries is also preceded by existing law. Norway passed a penal code in 1889, modeled after an 1866 Danish reform, which made invasions of privacy a criminal offense. Norway has a strong government welfare state policy; as does Sweden, its government maintains extensive central population statistics, and issues a personal identification number (PIN) as a matter of routine administrative efficiency. Hence, when that country focused on the issue of computers and privacy, it particularly explored the use of computer systems in its public administration. After eight years of drafting and discussion, the Norwegian Personal Data Act was passed in May, 1978.

There is an existing Norwegian public right of access to government files and the Data Act strengthens this to apply its general provisions to private computerized data banks, and both computerized and manual files in the public sector. The act also establishes a general principle of relevance: an "objective" rationale must be established between the registration of personal data and the legitimate goals of the collecting organization.

Norway's law is the first to define "personal information" to include data on "associations or foundations", a very broad category which extends protection to legal persons. Consequently, corporations have the right to access records maintained on them by banks, clients, and even competitors. This liberal interpretation was included in the act because the Ministry of Justice contended that the maintenance of a distinction between "persons" and "enterprises" would create a loophole for "mixed" registers to escape compliance.

Significantly, the law also creates the requirement of an "export license" on data to be communicated outside Norway. There is also a clause which provides the option for Norway to enter into cooperation with countries having agencies similar to the Data Surveillance Board. This clearly accounts for international solutions to the transborder issue.

Separate private and public sector data laws were adopted by Denmark in May, 1978 effective 1 January, 1979. They create a privacy agency, the Register Board, with enforcement powers over industry and the government, with each subject to different standards

[9] U.S. Department of Commerce, National Telecommunications and Information Agency, "Swedish Data Act", "Selected Foreign National Data Protection Laws and Bills," Special Publication, ed. Charles K. Wilk (March, 1978).

and controls. The laws encompass the regulation of transnational data traffic as well as purely domestic operations.

The registration of certain information is conditioned on its "relevance" to the purposes of the public or private organization, and both laws contain consent provisions for the transmittal of sensitive information to third parties. It is pertinent that while the public sector law protects only computerized systems containing personal information, the private sector law is somewhat broader, taking account of computerized data bases and any other type of "systematic registration", and extending protection to financial data on legal persons. However, the general right of the individual to inspect his or her own file applies only to government systems.

The Register Board acts in a supervisory capacity to the establishment of new systems in the public sector, insuring that each system conforms to a set of standards geared to the legal requirements; and it also has broad powers to inspect public record systems. In the private sector, the Register Board has more actual decision powers; for instance, it may enforce a minimal system of licenses and registrations. If a private system infringes on the substantive rules of the act, the injured party has certain rights of appeal to the agency.

The law on private systems subjects data processing or storage in foreign computers to licensing. This requirement obtains, however, only if sensitive information is included in the foreign record. Private systems that send data abroad for computerized processing must also comply with such provisions as insuring data security and correctness, and the deletion of outdated information. These rules are operational if the subject company is either incorporated in Denmark or if its information concerns Danish citizens.

3. West Germany

The data protection bill which was drafted by the West German Federal government in 1971 was intended for areas of privacy protection which were not yet covered by already existing special laws. Public hearings on the bill focused mainly on the regulation of public data banks, apparently because the computerization of personal data in this country is less advanced and conspicuous in the private sector than in the government (for example, the federal government controls an extensive population register). However, the German Federal Data Protection Act does cover the complete sector of private business, including such enterprises as banks, insurance companies, stores, and factories, as well as trade unions and political parties. With some exceptions, its scope includes manually handled files as well as electronic or computerized data bases. The processing of personal information is generally forbidden unless the person concerned has expressed consent or unless allowed under an exception to the act. A federal comissioner has overall responsibility for ensuring compliance in the federal administration. He or she maintains a list of all automated data banks containing personal data, and has the right to inspect all data banks. Private businesses that employ at least five persons in the course of automatic processing of personal data (twenty persons in the case of nonautomated data processing) must appoint a "data protection representative" who keeps a record of personal data stored and of the purposes for which they are required. Private parties who process data for the benefit of others are subject to simliar compliance stipulations.

"Personal information" is defined in the act to relate only to identifiable physical persons. Legal persons are not protected; and there has been no effort to grant them any rights of access or other protection of the act. The substantive rules of the law include the correction of personal data and the deletion of unneeded files; and the federal government is subject to detailed publication responsibilities to inform subjects of the contents of its stored data. The private sector must also inform persons concerned upon the storage of personal information; and there are access rights to both sectors. The Data Protection Act was adopted in November 1976, and went into effect in January 1978.

4. France

Discussion of the need for general privacy protection principles was provoked in France in early 1969 by a number of government measures designed to establish specialized national registers. A commission on information policy and civil liberties was established in 1974 by the Ministry of Justice. Louis Joinet, a leading and very respected member of that commission, was appointed to draft the French privacy protection law. The commission's activities have been watched in earnest by the top American computer service firms, since they rival those in France, which are the largest in Europe.

The French law on Information Processing and Freedom has been effective since January 1978. It has come into force progressively, and will take full effect in January 1980. The law attempts to control data systems both operating within France and those transmitting any form of data across that country's boundaries. It established a National Commission on Data Processing and Freedom as an enforcement agency; and it applies equally to both the private and public sectors in terms of acknowledging the subject's right of access, the obligation to rectify wrong data, etc. The enforcement mechanisms to be applied, however, differ. The state or public sector, or private firms working for the public sector, must await a prior authorization resulting from a commission recommendation before their data bases may begin to operate. Prior registration is required of all firms or individuals operating name-linked information processing systems. The registration process is quite comprehensive and involved, as the information required includes the characteristics and ultimate purpose of the processing; the categories of people having access to the data; where the data comes from and where it may be sent; and what precautions have been taken to insure the security of the processing and to insure confidentiality. One clause particularly affecting foreign based firms or multinationals in France requires that the operator state that the processing will result in name-linked data being sent out of France.[10]

One of the most obvious issues to affect business interests during drafting of the bill was its treatment of legal persons. The original plan was to insure that proprietary information on legal as well as physical persons be protected. At first, the private sector favored this broad application, as it could have allowed disclosure of data held by state institutions. In its final form, however, the law covers only data bases which handle files of personal information. Two factors produced this result: first, some large firms with particularly comprehensive files on their competitors did not want them to be allowed access. Secondly,

[10] "Focus on France", TDR, vol. 1, No. 1 (March, 1978), p. 2.

insurance companies and the major banks realized that it would have been much more difficult to hold name-linked data on the small- and medium-sized businesses they deal with. Subsequently, the inclusion of legal persons in the bill was dropped with relatively little parliamentary debate.[11]

The Ministry of Justice opposes this exclusion of legal entities because, among other reasons, it feels the law should contain a preference for the interests of the smaller business sector over those of larger firms and conglomerates.[12]

5. Great Britain

Britain, on the other hand, has proceeded very cautiously in drafting privacy legislation. The Committee on Privacy under the Parliament, chaired by Kenneth Younger, published in 1972 a document entitled the "Younger Report". It was ambivalent about the creation of a general right of privacy that might conflict with rights to freedom, speech, and communication. This is one reason why British legislation has been so slow in forthcoming. Meanwhile, a Data Protection Committee was established to explore alternatives, and it published legislative proposals in December 1978. The report recommends the registration of personal data systems of the government and some private organizations, and the preparation of some fifty codes of practice for particular private sector applications. Only the automatic handling in the United Kingdom of personal data would be covered in any such legislation, and compliance would be handled by a Data Protection Authority.

Several recommendations were detailed to accommodate transborder data flows. These include the protection of all nationals of other states as well as British citizens, compliance with the data authority by foreign entities operating in the United Kingdom, and the inclusion in the code of practice of any regulation of transborder transmission as may be necessary to insure compliance with the code. The report clearly advised the United Kingdom to avoid being denied the normal flows of information, as it also emphasizes that the government play a positive role in current negotiations for any international data protection convention.[13]

6. United States

Finally, American agitation on the topic dates back to the early 1960s. Since the United States had been ahead of Europe in its computer development, its impact was also felt sooner. Interest was at first instigated by the prevalence of government data processing systems; and shortly turned to systems in the private sector. Six major privacy related laws have been enacted since 1966.[14] While their enforcement methods do not include registration or licensing procedures, they confer rights of public access to government records pertaining to its activities and personal data on American nationals. Also, conditions are placed on the dissemination of personal information by the government and select private industries. Also legislated is

[11] Id., p. 3.
[12] Louis Joinet, "French Law in Relation to Information Privacy", Transnational Data Regulations: European and Third World Realities, Online Conference (New York, Nov. 28–30, 1978).
[13] "British Data Protection Report Published", TDR, vol. 1, No. 7 (November 1978), p. 11.
[14] For a summary of the United States privacy laws, see U.S. House of Representatives, Committee on Interstate and Foreign Commerce, "The Impact of Communications Technology on the Right to Privacy", *Options Papers*, 95th Cong., 1st sess. (May 1977).

the interception of electronic communications by the federal government for purposes of evidence in criminal proceedings. A number of privacy-related study commissions has been established by federal law, among which was the Privacy Protection Commission established by the Privacy Act of 1974. Its purpose was to recommend extensions of protection standards established by this law for records held by the federal government to those held in the private sector. The Commission's report was issued in June 1977, and related to record-keeping practices in a number of fields, such as insurance, banking, credit and employment.

C. TRANSBORDER DATA FLOWS

1. Major Issues

The majority of European countries which have enacted or are considering privacy legislation domestically are seeking to extend these protections to data transmitted and processed outside of their boundaries. The protection of personal privacy is only one aspect of this interest. This is an important objective, since in the absence of a treaty, data protection regulations have no legal effect in other countries.

However, all kinds of data are involved, not just those that affect the individual. Observers note a need to mediate among standards that form the basis of proposed European data restrictions, to be applied for purposes beyond the micro level of personal privacy.

Both private enterprise and public authorities there perceive economic and technological effects of international competition in hardware and services. The export of data abroad is induced by the attractive terms and the flexible range of services offered by commercially mature businesses. This flow of local revenues to established foreign services is often accompanied by capital, investment monies, and talent. While domestic users come to rely on transborder data flows, the home industry may flounder at the outset, or simply die out. The application of standards and sanctions on these flows could promote more local processing of data for service to old markets and to stimulate new markets as well. The multiplier effects resulting from the boost in local employment and technology would redound both to a country's economy and its international balance of payments.

This is also a matter of possessing resources suitable in an "information age". An explicit premise is that it is necessary to study information as a production factor in the post-industrial era. Commercially, there is a perception of dynamic expansion in the field. The legislating of data barriers is becoming a matter of international prestige as well as judicious economic planning.

All of these standards—the protection of individual privacy, the development of the local economy, and the fear of being left behind as others reap the benefits of a crucial asset—bespeak of a natural desire for defense against vulnerability and for freedom from external control. Politically, this is a matter of national sovereignty. National defense is one crucial element of the various rights and obligations that derive from this concept.

There has been some sense of foreboding from those who discern impacts of transborder data flows on military preparedness; at any time, vital segments of a country's data mass may reside abroad. Sweden in particular is an agitator on this issue. National security

may be vulnerable if the free transmittal of data is not guaranteed, and if the home country is not assured of purview. The Swedish Ministry of Defense established a committee in 1977 to investigate and report on the "vulnerability of a computerized society," and to propose corrective measures. It has pointed out that more than 2000 systems containing personal data on Swedish citizens are located in other countries; [15] and the element of risk deriving from the high concentration of computer capability in the Stockholm area. This convergence is apparently coupled with an absence of alternate back-up systems. The committee regards this arrangement as a threat to the public order should an accident or sabotage occur, even in peacetime.[16]

Canada and Japan are also turning to the question of where computerized data bases and services reside which contain information critical to the functioning of the countries' industry and government. There is genuine fear of real economic losses resulting from maintenance of Canadian data in the United States. There are "in Canada" record storage requirements in both provincial and federal legislation. For instance, a medical information file owned by insurance companies in the United States has been obliged to establish a Toronto subsidiary to keep Canadian data.[17] The Canadian government's position was reiterated at a conference on Issues in Canadian-United States. Transborder Computer Data Flows conducted in September, 1978 and sponsored by the Montreal-based Institute for Research on Public Policy.

It is estimated that Japan is about ten years behind the United States in data base sales and applications. The concern there is that if its lag in the software sector continues, it may become completely dependent on American information service firms.[18]

National sovereignty may also be perceived as an assertion of "identity" in the generic sense: the distinguishing characteristics of an individual, or on the level of the community, of a collection of individuals. A national identity constitutes an objective reality in the eyes of its members and of outsiders. This reality is made up of particular habits of thought, modes of behavior, and measures of social power. It is felt that the use of data processing across national boundaries can bring about "the homogenization of cultural tastes and attitudes. . . . (t)he process that each country goes through to attain this homogeneity may be different and in some cases lead to social upheaval." [19] Parallels are drawn to data processing from the significant cultural effects that are widely recognized in broadcasting. Regulation is regarded as the answer to such social consequences.

American dominance in the data communications and processing industry accentuates these concerns. Apprehension that bear on the protection of personal privacy have major implications for the status of American law and for the conduct of American business abroad. Those laws presently on the books—the Fair Credit and Reporting Act, the Privacy Act, and so forth—do not extend protection to the

[15] Angeline Pantages and G. Russell Pipe, "A New Headache for International Data Processing", Datamation, vol. 23, No. 6 (June 1977), p. 118.
[16] TDR, op. cit., n. 7, p. 17.
[17] Pantages and Pipe, op. cit., n. 15.
[18] "Japan to Begin Study on Purchase of America's Advanced Data Base", TDF News, vol. 1, No. 3 (October 1978), p. 4.
[19] OECD, Data Bank Panel, op. cit., n. 2, pp. 10-11.

nationals of other countries who may be living or traveling within the United States. Furthermore, while there are several proposals now pending in the U.S. Congress for extending more comprehensive privacy protection, much European law is advanced further beyond this stage. This instills fear on the part of American multinational users that the amount and types of personal information collected and stored in their networks may be severely restricted for lack of reciprocity. American based computer communications firms could be likewise affected; and not only would they have to answer for their own in-house systems, but also they would face an enormous shrinkage of markets. A loss of business of all kinds may occur that might not be recouped even in the long term. Much the same commercial effects would flow from restrictions grounded in any other standard of national sovereignty.

Consequently, a multinational would have to tailor the operations of its affiliates to suit the enforcement criteria of the laws of nations in which they are binding. Repositories of information may accordingly have to be transferred from centralized data bases. They would have to meet applicable license, registration, and other non-tariff requirements. Tariff barriers—the taxation of, or the placement of duties on data bases and networks—may also be used as an enforcement technique and/or to simply generate revenue. PTT's in England and France, for instance, have been placing a surcharge on access to U.S.-based systems. Any of these enforcement techniques may compel U.S. data base vendors into the position of having to negotiate with state-controlled common carriers or a monolithic European monopoly in the form of EURONET.

Thus, serious economic implications are based on seemingly innocuous and reasonably enlightened motivations, which are discerned as mere pretexts to shut out extraterritorial companies. This situation has been labeled as the first skirmish of an "information war." In this view, barriers are aimed explicitly at American companies, since they take up the lion's share of foreign revenues in information technology and expertise. It is observed that modern data communications is threatening to eat into the business of public utilities, as well as private vendors. The institutional and political strength they can muster could force the invoking of sovereign powers. This could also be aimed at American multinational users whose dominance in certain industries such as hotel management and banking distresses foreign governments. Commercial development may create a lucrative market for selling information resources at a premium to developing countries.

While not always clear, these motivations are inferred from the effects of tariff and non-tariff barriers. It must be emphasized, however, that the United States has an interest in protecting the privacy of its own nationals, as unsafeguarded files on American citizens could exist in the absence of some form of extraterritorial application of U.S. law. The passage of liberal privacy laws in other countries would protect American travelers and nationals having any kind of business overseas.

A more universal apprehension is that of the chaos which can result from too many disparate laws. The many discrepancies among national laws make harmonization both desirable and difficult to achieve in practice. Governments with parallel interests in privacy and trade protection are recognizing that they have sufficient motive for accommodation that may not be assessed until damage is done. Also, eco-

nomic analysis is incomplete concerning the cost of data protection and the productivity of international data flows. Conventional assumptions of protection may not always apply. Much of the economic advantage depends on the economies of scale afforded by expanded computer and communications capacity. Hence, the erection of trade walls might not provide the needed incentive for domestic industry and service bureaus to develop: data barriers may prove to be a break on computerization. The only accomplishment of such regulation, then, could be an absence of modern service, a "data backwater".

There may, furthermore, be trouble in enforcement and in policing possible violators. While statutes may give some direction to commercial development, they cannot guarantee that enforcement methods will suffice for the data needs and hardware that will proliferate in any case. An aspect of this problem is the elaborate methods that may be devised for evading restrictions altogether. "Data havens" and "data piracy" are seriously discussed as the more pernicious results of unduly restrictive laws.

Data havens, like tax havens, may proliferate as users from countries with strict regulations move their operations to locales having either no law or very liberal practices. A Swedish firm that keeps its data on foreign soil therefore could reside in a data haven not subject to Swedish law. The United States, by virtue of its mature computer industry, is a particularly attractive data haven. Not only does the United States have no relevant privacy laws affecting the conduct of private industry, but it is also a source of cheap and reliable technical support for computing and teleprocessing.[20] Representative Barry M. Goldwater, Jr., foresees that individual nations or powerful financial interests could deliberately implement a data communications service operation that would have as its sole objective the circumvention of various national information statutes.[21] There is apparently some practice of "data piracy", although no one seems to know the extent or seriousness of the situation.[22] As a breach of information security efforts, there can be profit and minimal risk in the practice of signal interception and translation. Resale value would pertain to trade secrets, information on employees, clients, and credit, as well as the content of computer programs. This prospect, of course, unnerves heads of companies and states that process or store any part of their data abroad.

2. Action in International Organizations

Because of the magnitude of these information policy considerations, European countries are turning to international organizations for guidelines on national legislation and international cooperation that would balance interests against each other. This last consideration is one operating premise for discussion in OECD:

> In addition to economic, social and political consequences, transborder data flows are creating new forms of interdependence among countries. These developments in international data communications imply new obligations on the part of countries utilizing such technological accomplishments. Among them is the promotion of domestic policies and practices which will give a maximum of unre-

[20] Mark Porat, "Communications Policy in an Information Society", Communications for Tomorrow: Policy Perspectives for the 1980's, ed. Glen O. Robinson (New York: Praeger Publishers, 1978), p. 53.
[21] Barry Goldwater Jr., "Data Havens: International Privacy Threat", Computer Decisions, vol. 9, No. 6 (June 1977), p. 23.
[22] Id., p. 22.

stricted and uninterrupted flow of information, provide for competition in processing in the assimilation of data, and to insure individual liberties are respected.[23]

To reiterate, the task of the international organizations is to baiance the goals of respecting states' interests in restrictions with the assurance of the benefits of free flows of information across borders. This analysis of competing goals is obvious as an extension into international agreement of the same obligation on the part of domestic privacy law.

It is acknowledged that developments in international computer/communication networks can accelerate economic and technological progress in countries where they are connected. Specific national interests, however, can override the perception of this assessment. While discrete information markets may not in themselves be large, the conglomeration of restrictions has a potential for disrupting information flows and the economic activity which depends on it. At the same time, though they may be restrictive, there may be very valid proposals for protecting confidential information. It is the ultimate function of any data regulation to both reenforce and restrict the accessibility of information.

Since applying data transmission and processing to their own activities in such fields as health services, weather forecasting, and research, international organizations have been devoting special attention to the impacts of telecommunications. They have taken more initiative as Europe's governments have turned to these organs for effective action in dealing with the difficult transborder problems. Inevitably, these diverse activities have left some problems of overlapping not only among the various organizations, but also among the different departments within the same organization. Nonetheless, the following is a brief review of the major entities and their work.

(a) The United Nations

An inquiry was undertaken in 1968 by the Secretary of the United Nations on privacy problems; and a number of reports was subsequently furnished to the Commission on Human Rights. They recommended minimal international standards for the protection of personal data in electronic systems. While legal and administrative cooperation and technical and economic issues have been the points of departure for regional organizations, the United Nations, with its global perspective, has been preoccupied with the human and social problems caused by the advent of data processing and communications. It is also considering the attainment of communications technology on the part of the third world. The Commission's activities since 1974 have encouraged national attention on data protection. However, its recommendations and resolutions are left to the states to judge for themselves the compatibility of their practice and legislation. The option mechanism owes to the fact that different societies and political regimes are inclined toward varying notions of privacy and mechanisms of control. Consequently, the inquiry conducted by the U.N. has had no direct effect on public policies in any country.[24]

[23] OECD, Data Bank Panel, op. cit., n. 2, p. 14.
[24] Id., p. 42; Hondius, op. cit., n. 8, p. 61.

(b) Nordic Council

While the Nordic Council is not technically an international organization, it has as an official association compiled a substantial record on data flows and data protection. Its member states (Denmark, Finland, Iceland, Norway, and Sweden) requested the Council to recommend formal measures for electronic data processing and communications in 1972; however, consensus was not achieved on uniform draft legislation. The Ministers of Justice of the Nordic countries initiated a joint working group in 1975, in order to propose measures to harmonize the privacy legislation of the member countries. The working group summarized its findings in a report submitted to the Council in February 1977. It recommended the adaptation of national laws to establish a framework of minimum protection standards for continued data transmission among the Nordic countries, while also opening the way to mutual administrative collaboration. It was felt that any attempt to enact uniform legislation would infringe on either the relative freedom of transmission or the protection requirements that have already been proposed or implemented. It was advised that the Council resume its work when laws have been adopted in all of the member countries.

Activities in the Nordic Council are being watched with interest by other bodies as precedent for international agreement; and the membership of the Scandanavian countries may be pivotal to the logistics of OECD and the Council of Europe (Denmark is also a member of the European Economic Community).

(c) Council of Europe

The purpose of the Council of Europe is to achieve unity among its member countries through conventions and agreements on matters on which they share common interests. The geographic scope of the Council constitutes 19 states located in Europe, and other countries are sometimes admitted as observers to its proceedings. The Council of Europe has had since 1968 a range of activities on the use of data processing and communications, inclusive of guiding states on their privacy legislation; and it established a committee on Data Protection in 1971. The Committee has since 1974 been dealing with the formulation of resolutions on the protection of data banks. In 1976, a new committee was established to pursue issues related to international data flows. While it is currently revising a draft bill submitted to it by the Council's Legal Affairs Committee, this bill is to be the basis of sponsoring an International Convention on Data Protection, and is expected to be circulated to member countries in early 1980.

The Council of Europe's bill concentrates exclusively on the protection of personal data across borders, without discussing the effects of these flows on other levels of concern. It seeks to establish common rules among nations on the right of the individual when an automated record is gathered, processed, and transmitted across borders, and to solve jurisdictional conflicts that occur when information is compiled in one country and processed or stored in another. Each signatory would apply the resolution's standards domestically through the oversight by a central data authority of the information processing and transmission industry. The bill also states that data processing systems must conform to security standards over equipment as well as data.

(d) European Ecomomic Community

A working group was formed in the EEC in 1976 to review privacy legislation produced by its nine member states, and to see to what extent an overall draft agreement is appropriate. The group was formed out of a concern that "data havens" would result from legislation produced by any of the member countries. By imposing a community norm, a "free data zone" could be established. Further basic requirements could be set to govern transmission to non-member countries.[25]

Early in 1978 a conclusion was reached to await completion of the preliminary draft of the convention proposed by the Council of Europe before determining what form of legislation should be proposed with the European Community.[26]

(e) Organization for Economic Cooperation and Development

The membership of the OECD is comprised of 19 European states, Canada, the United States, Japan, and Australia, a cross-section of countries on four continents with similar political, economic and social systems. The organization's work on information policy dates from 1969. A Computer Utilization Program was conceived at that time, the outcome of which was the commencement of study in 1974 of the transborder data flows issue by a Data Bank Panel. The Computer Utilization Group was consolidated with the Information Policy Group into an Information, Computers and Communications Policy Group (ICCP). This is an effort to centralize activities which fall under the broad umbrella of information policy, including transborder data flows.

OECD has conducted about the most comprehensive treatment of the data flows issue in an international body. The Data Bank Panel prepared a first tentative draft on the subject in January 1977, for circulation and comment. Substantial research was prepared for this draft by the Computer Utilization Group.[27] The document notes the interest in the protection of personal privacy and the many different rules which may have the effect of obstructing data movements, although it does not stipulate standards in the context of privacy. Instead, it focuses on the economic and technological aspects of the data flows issue. This approach differs fundamentally from that of the Council of Europe. The Data Bank Panel notes: "It has now become clear that the concern over the protection of personal data, while the important catalyst for past efforts, is not easily isolated from the general development of trans-nationalization of information systems of all kinds." [28] The group recommends "multilateral action",[29] presumably to incorporate a balance of interests into an explicit agreement.

To this end, OECD sponsored in 1977 a Symposium on Transborder Data Flows and the Protection of Privacy, in conjunction with the European Economic Community, the Council of Europe, and the Nordic Council. The symposium brought nearly 300 participants to Vienna from international organizations, government, and

[25] "Common Market Seeking Common Privacy Policy", Computerworld vol. 11, No. 8 (Feb. 21, 1977), p. 11.
[26] Frank Carmody, "The Work of the European Community in Areas of Computers and Privacy", TDR, op. cit., n. 12.
[27] See, e.g., above, n. 3.
[28] OECD, Data Bank Panel, "Preparation of a Symposium on the Transborder Movement and Protection of Data," mimeo (Paris, Jan. 14, 1977), p. 2.
[29] OECD, Data Bank Panel, op. cit., n. 2, p. 6.

private firms, including about 30 observers from the U.S. Government and private sector. This representation provided a broad perspective for discussing the transnational privacy protection issues, taking economic and technological aspects into account as well.[30]

Subsequent to the Vienna Symposium, early in 1978, OECD created a new expert group on Transborder Data Barriers, with the purpose of drafting guidelines on the issue by July, 1979. There are two main elements to this task: While the guidelines are to be a basis for harmonizing personal data and privacy, the group will also explore the legal and economic problems relating to the transmission of nonpersonal data. Guidelines would then be drafted for this area, taking into account the principle of free flows information. Cooperation is taking place between the Council of Europe and OECD to insure that these directives and the Council-planned international convention are drafted in similar fashion and do not conflict with each other.

IV. Framework for Future Consideration

While the U.S. Government has been devising its own domestic privacy stance, it has not taken a leadership role in global developments. A position is being considered in an interagency task force established in the State Department in December 1976, of which representatives of the National Telecommunications and Information Agency, the Office of Management and Budget, and the Federal Communications Commission are members. There is also a Public Advisory Committee on Transborder Data Flows, in which a subcommittee was formed in late 1977 to develop awareness of the issue in private industry and trade associations. It has also worked with the interagency task force to critique proposals from overseas.

It has been pointed out that while many other industrialized nations are devoting direct governmental attention to data flow issues, to the extent that the Council of Europe is close to finalizing a draft multinational convention, U.S. discussion and activities are "occurring without any meaningful Administration support, without any clear Congressional mandate or support and without any agreed-upon goals."[31] Until recently, many corporations were not aware of developments in transnational data regulation. In a mid-1977 survey on the subject conducted by Datamation magazine, and directed to Fortune's top 1,000 U.S. companies, only 40 responses were received from companies that had foreign data processing operations. The reaction of most was confusion about their requirements affecting transborder flows.

There have been concerted discussions more recently in the context of several conferences on the issue. In one major session, conducted in New York in November 1978, several computer users criticized both the U.S. Government and the business management community for not fully appreciating the scope of the transnational data flow problem.[32]

---

[30] For a discussion of the conclusions developed at the symposium, see H. P. Gassmann, "The Activities of OECD", TDR, op. cit., n. 12.

[31] "Goldwater Calls for Conference on TDF", TDF News, vol. 1, No. 3 (October 1978), p. 2.

[32] "Users Blast U.S. Inaction", Computerworld vol. 12, No. 50 (Dec. 11, 1978) p. 2.

The following is a list of issues which provides a framework for assessing proposals before the Council of Europe and OECD. The first several issues relate to the question of international regulatory standards for the operation of bases and networks:

(1) Should standards be established in national legislation or international agreement, or both?

What would be the effect of either of these options on competition in international data processing and transmission markets?

(2) Should standards be strict—requiring licensing and close regulation of the market, and covering data generally that transits political boundaries, or permissive—providing standards and limited in scope only to personal data?

In either case, what would be the effect on international data markets?

(3) What mechanism would be conducive to the modernization of information services in developing countries?

The second set of questions addresses the need for balance between privacy considerations and the free flow of data across boundaries:

(1) Should the United States seek the extension of personal privacy protection abroad?

To what extent is personal privacy endangered by the absence of internationally agreed-upon protection?

(2) What obligations should the United States assume to guarantee rights of privacy and information to foreign nationals in accordance with standards acceptable abroad and consistent with their national laws?

○